Hunting code injection with Sysmon:

Here we will learn how to use sysmon to detect the creation of remote thread in a process.

We will open Event Viewer and then go to the Sysmon logs. In “Application And services > Microsoft > Windows > sysmon > operational”

One thing to note, the sysmon will log things that are in the Configuration file we give it:

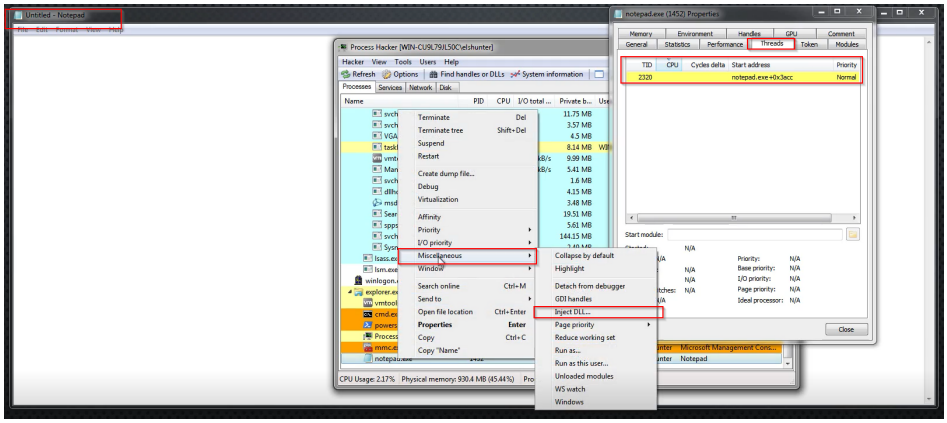
Here we will open the notepad and then inject a DLL into it and then we will check the Sysmon logs:

We can use Process Hacker which is a tool to monitor the Process but we can also use it to inject dll into a process.

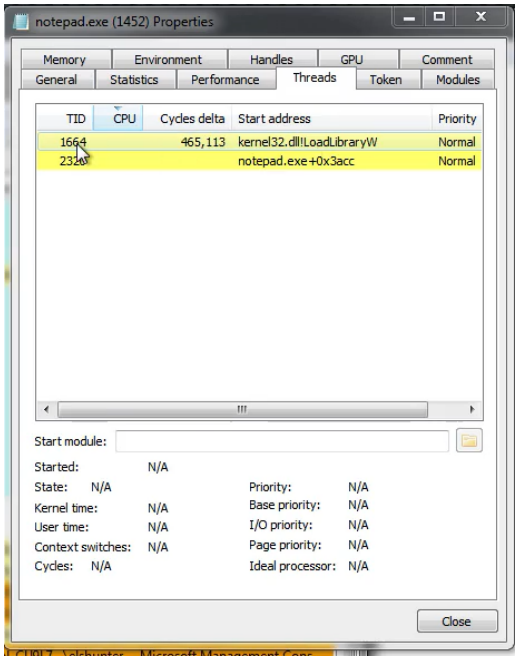
One thing we know that when an application or software is launched it will load the DLLs so it can run, and the DLL injection is a normal behavior to happen to the running process, mean the developers will use the DLL injection technique to like extend the functionality of the program, so that mean the DLL injection it self is not malicious but can be used for malicious purpose.

DLL injection is performed by the malware so it can take over a legit process and then use that legit process for malicious way so it can do the malicious things without to get detected

We will go the properties of the notepad.exe in the process hacker tool and then we can go to the modules to see the DLLs running for the notepad.exe but we will go to the threads and then we will right click the notepad.exe process and then go to the “Miscellaneous > inject dll” to inject a dll.

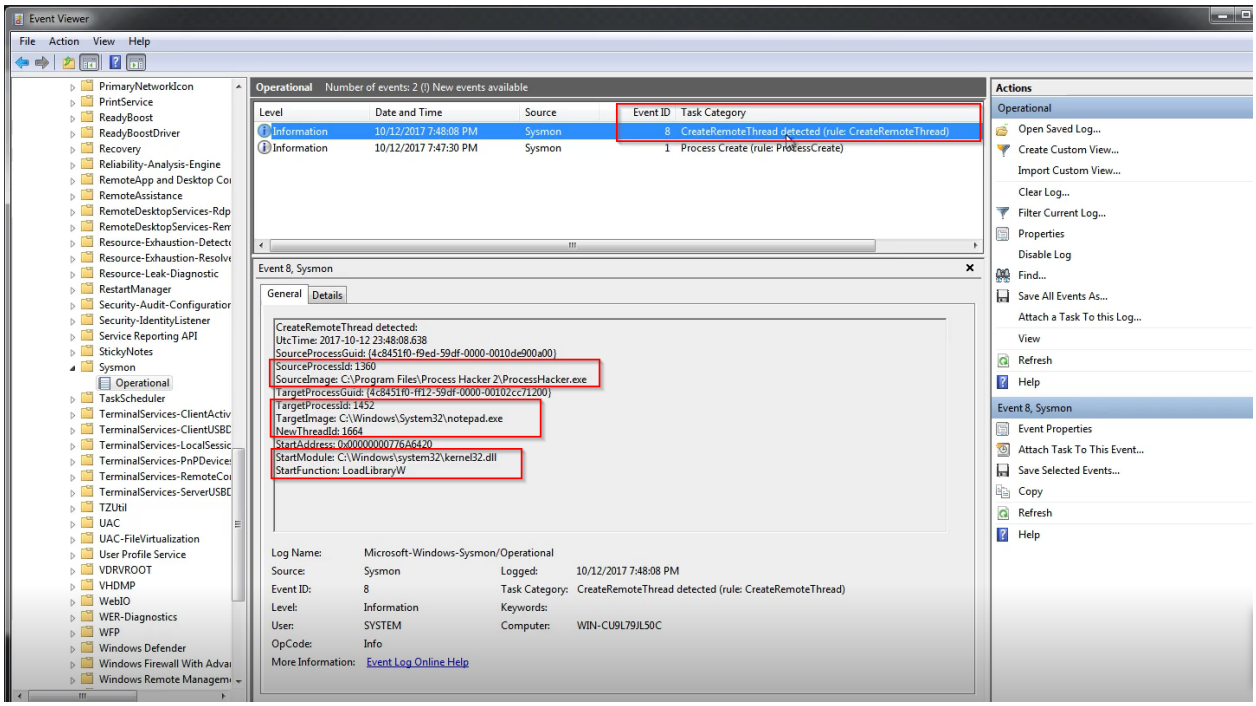


Then we select the DLL that we want to inject into the notepad.exe process.



After injecting the DLL we see a new thread with TID 1664.

Lets go the sysmon logs in Event Viewer



Here we see the Event ID 8 which is for new thread created and we see the Event ID 1 this is when we launched the Notepad.exe but we will focus on the Event ID 8:

We see the source process ID and the source process Image that did the injection mean the process that did the injection had ID 1360 as we see in the SourceProcessId: 1360 which is the ProcessHacker.exe that

we used to inject the DLL, and we see the Targeted Process image and PID which is Notepad.exe, mean the ProcessHacker.exe with PID 1360 injected into notepad.exe that has PID 1452 and created a new Thread with ID 1664.

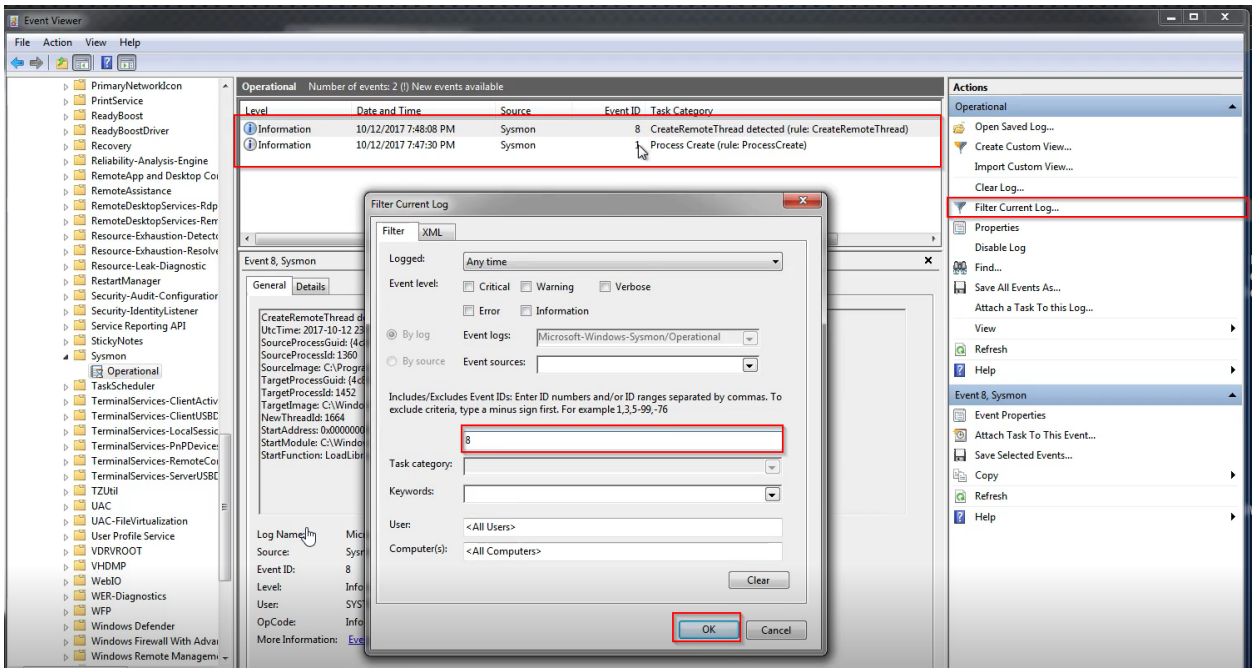
The Module that used to inject the dll was kernel32.dll , that's how we know it was a DLL inject and we see the function "LoadlibraryW"

We can also use PowerShell to get the Sysmon or any logs from the Event Viewer using the "get-winevent" cmdlet.

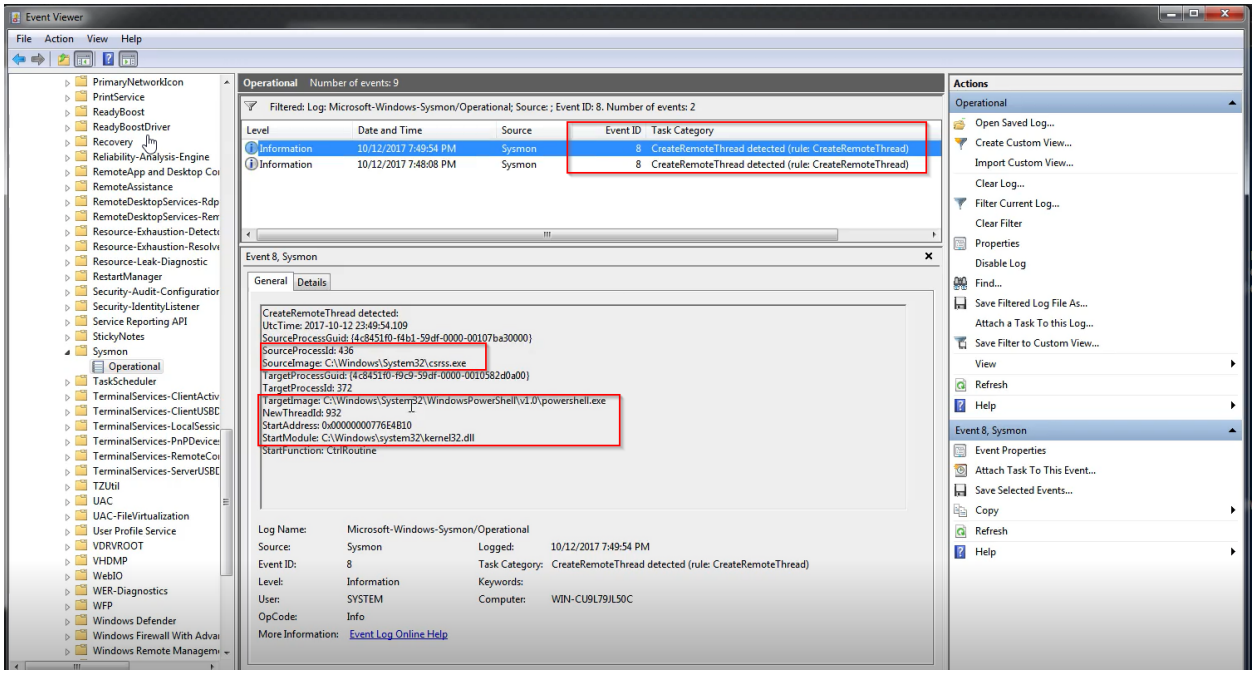
Using the command by it self will return all the logs so we need to add some filters, so we will filter for EventID 8:

```
PS C:\Users\elshunter\documents\sysmon> get-winevent -FilterHashtable @{logname="Microsoft-Windows-Sysmon/Oper
ational";id=8}


   ProviderName: Microsoft-Windows-Sysmon

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
10/12/2017 7:49:54 PM            8 Information      CreateRemoteThread detected:...
10/12/2017 7:48:08 PM            8 Information      CreateRemoteThread detected:...


PS C:\Users\elshunter\documents\sysmon>
```

Here we use the filterHashTable flag which we will help us filter but there is better and easy way to do that but here we see the 2 events and in the Event Viewer we saw one, lets do the same filter in Event Viewer to see if we get one or two:



The result:



Here we see the csrss.exe injected into powershell.exe which happened after we injected. Normally legitimate software processes like **csrss.exe** generally shouldn't be injecting code into other processes like **Powershell.exe**.